RSAC 2025 Conference

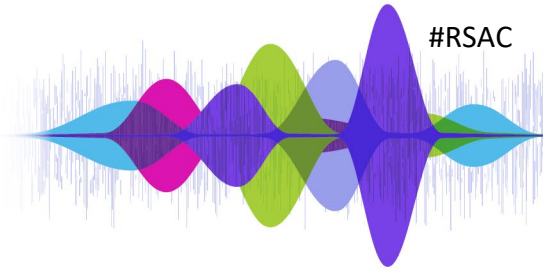
Many Voices.
One Community.

SESSION ID: USENIX-M05A

Terrapin Attack: Breaking SSH Channel Integrity by Sequence Number Manipulation

Fabian Bäumer

Research Assistant
Ruhr University Bochum

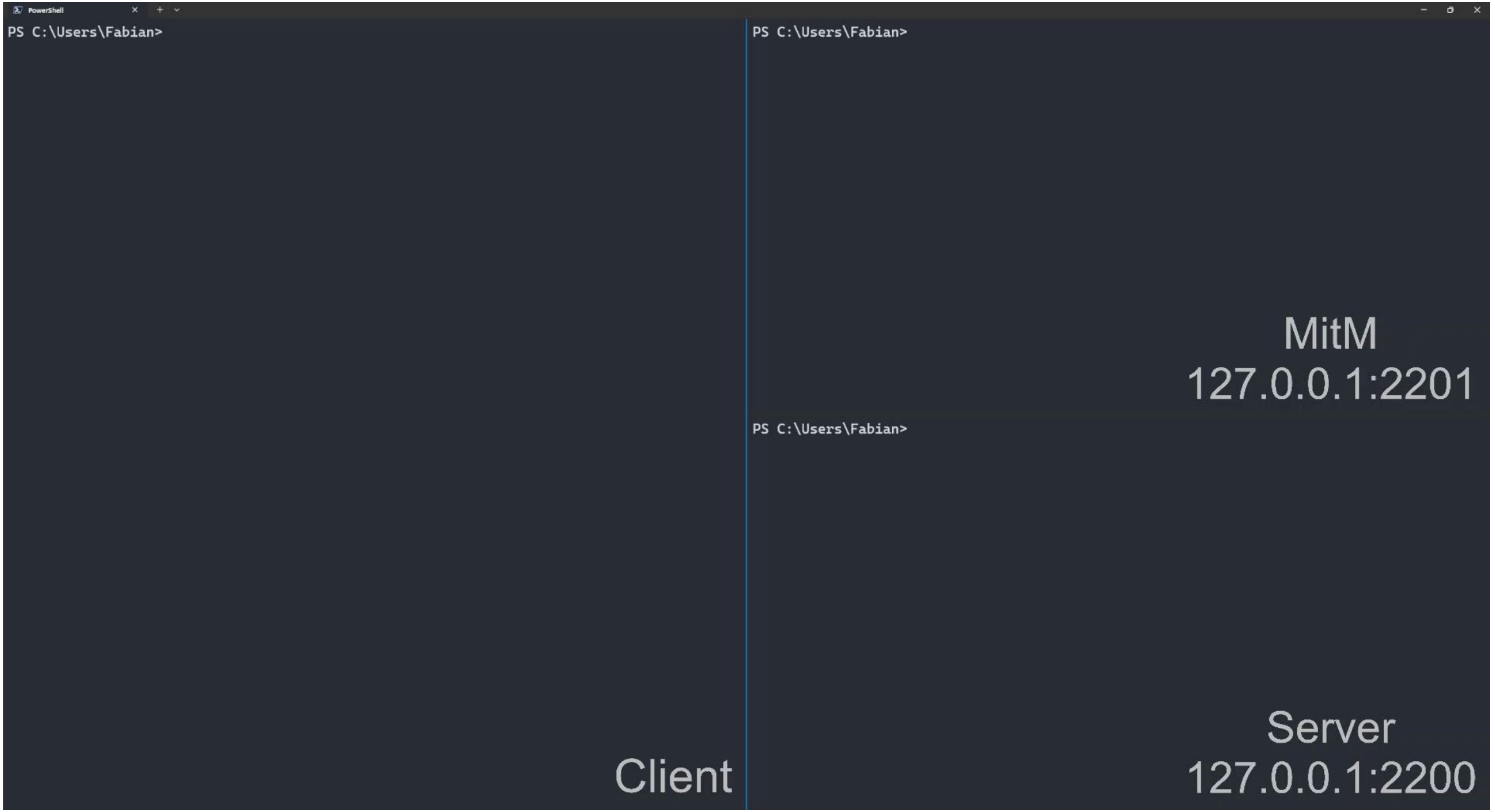


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.


PowerShell
PS C:\Users\Fabian>
PS C:\Users\Fabian>
MitM
127.0.0.1:2201
PS C:\Users\Fabian>
Client
Server
127.0.0.1:2200

RSAC 2025 Conference

The Secure Shell (SSH) Protocol

SSH Is Split Into Separate Layers

SSH Connection Protocol [RFC4254]

SSH Authentication Protocol [RFC4252]

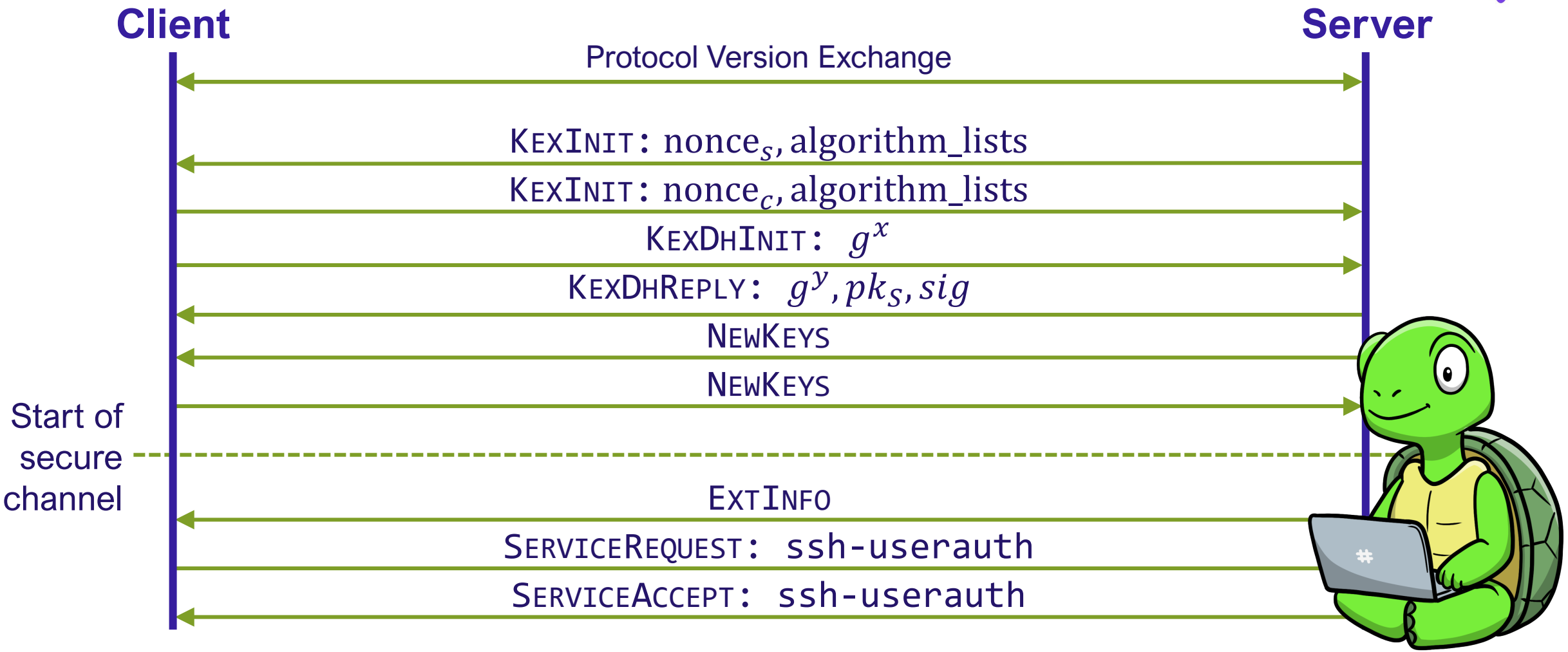
SSH Transport Layer Protocol (TLP) [RFC4253]

=> Binary Packet Protocol

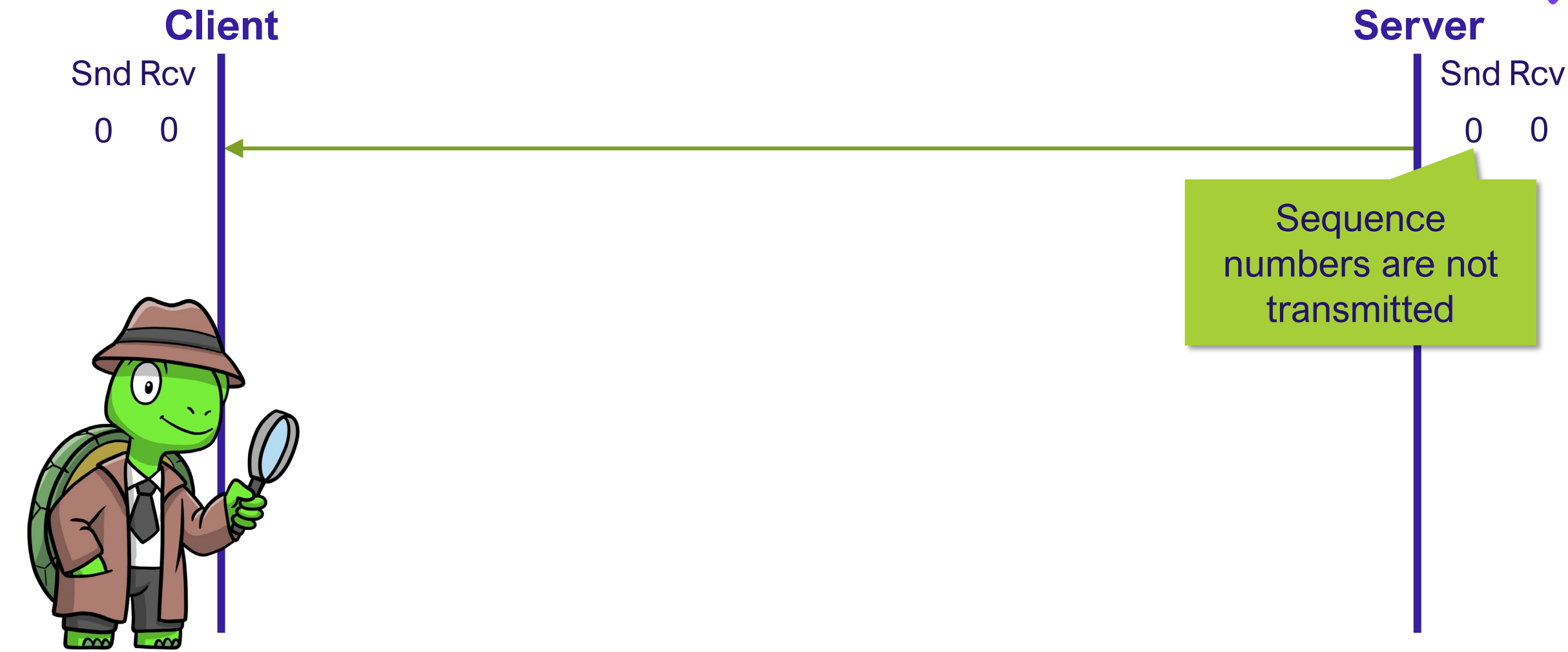
=> SSH Handshake

TCP / IP

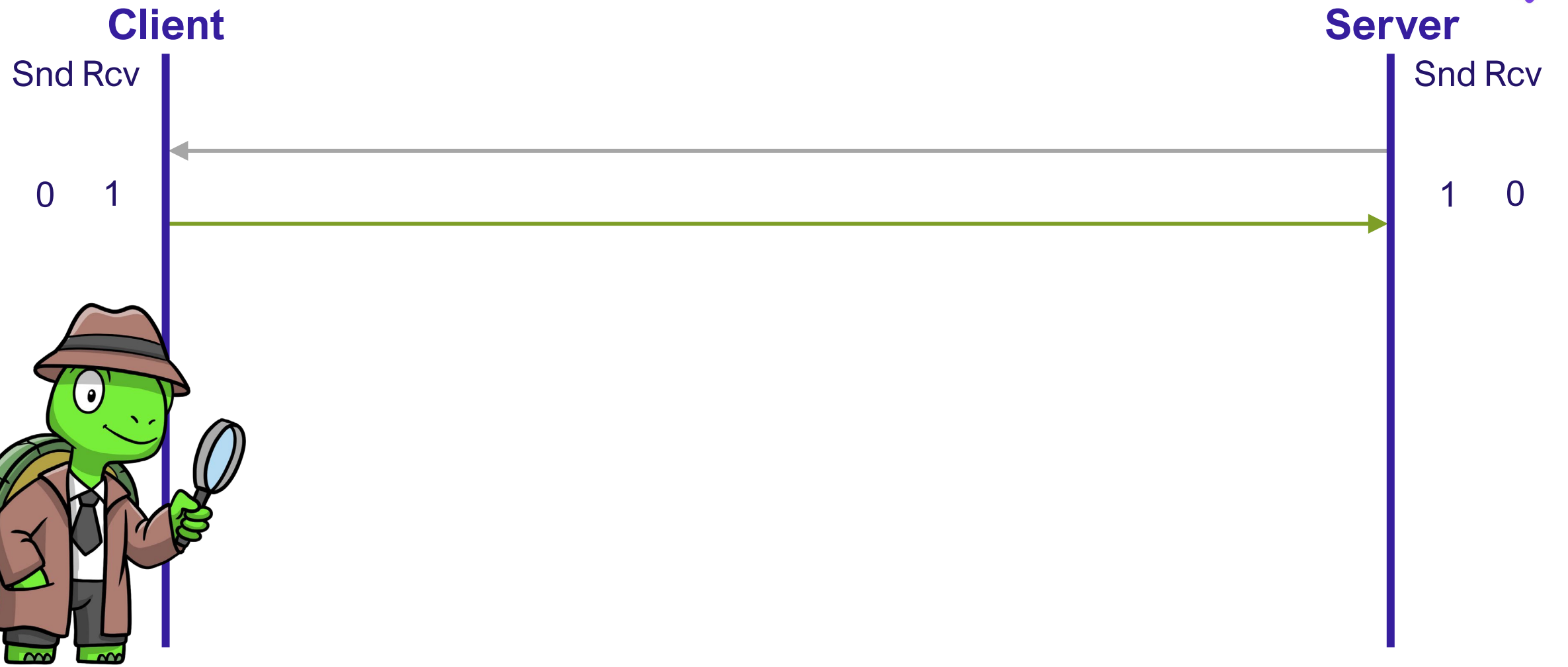
A Typical SSH Handshake



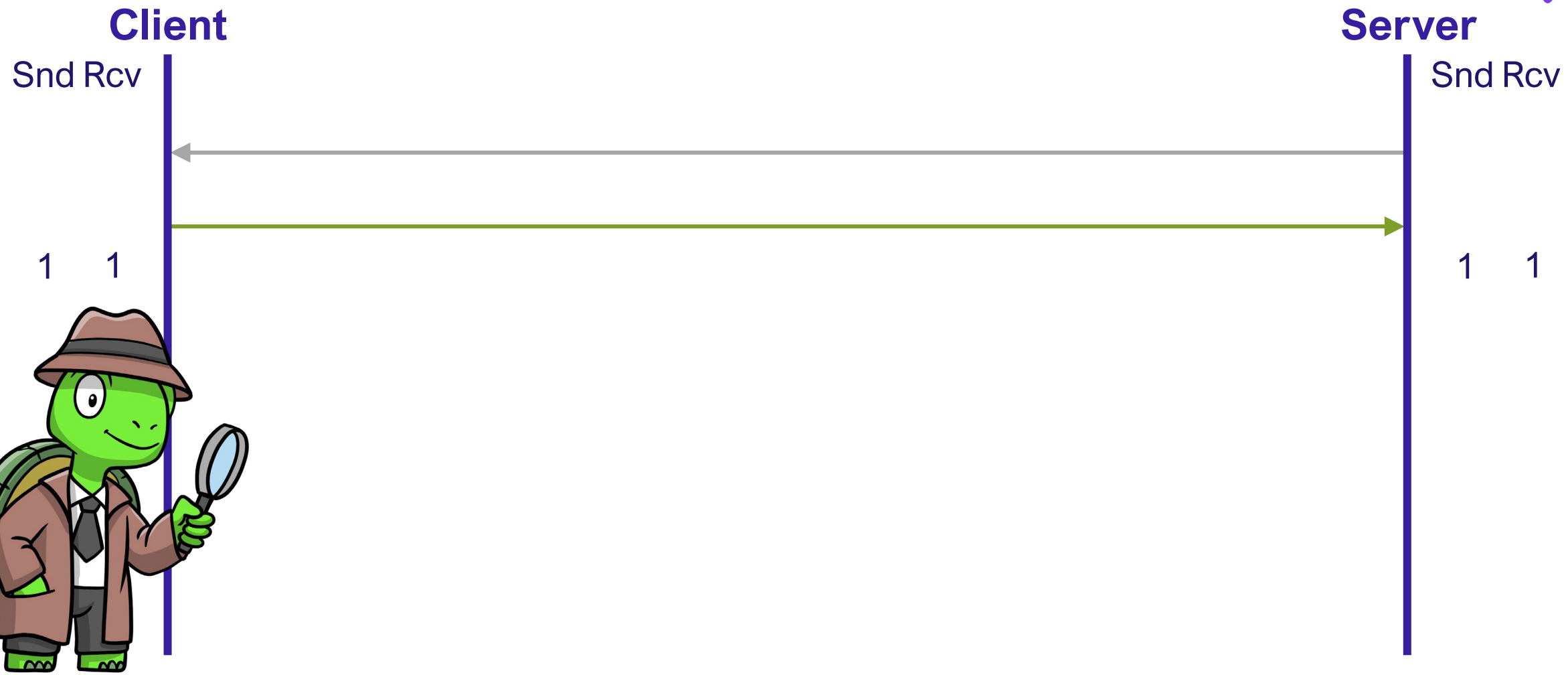
SSH Uses Implicit Sequence Numbers



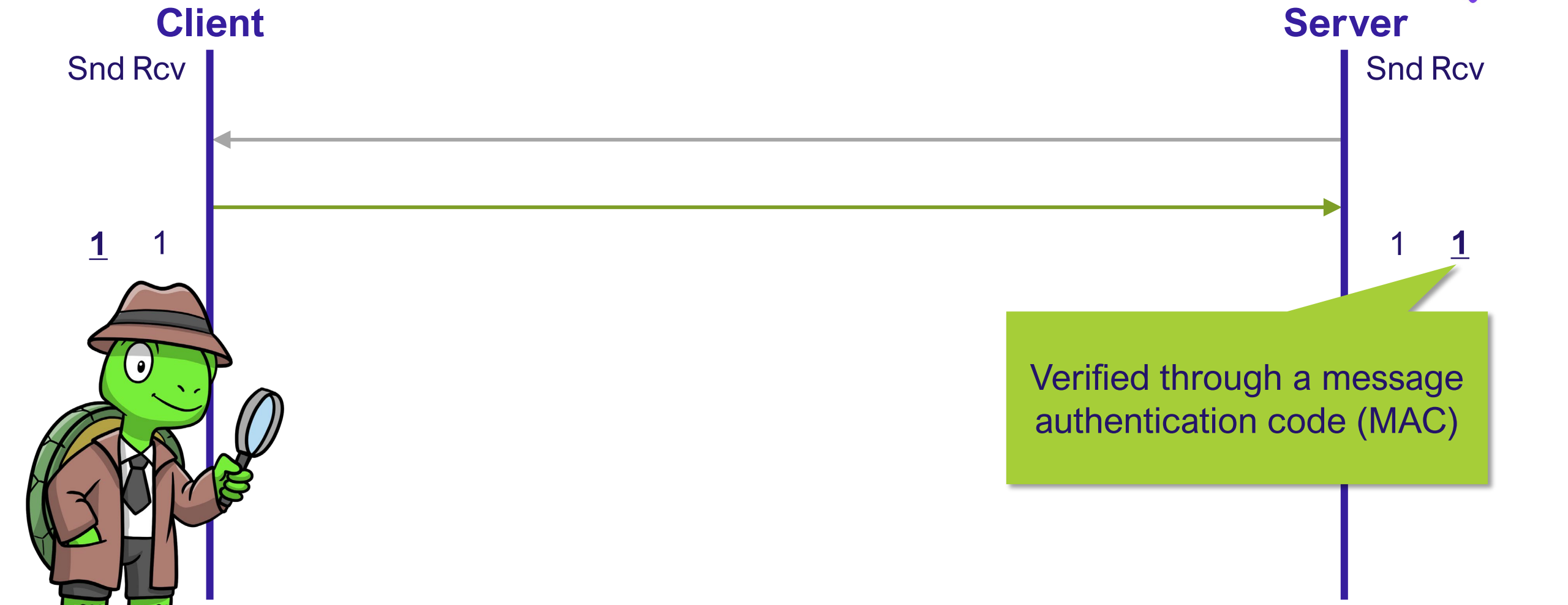
SSH Uses Implicit Sequence Numbers



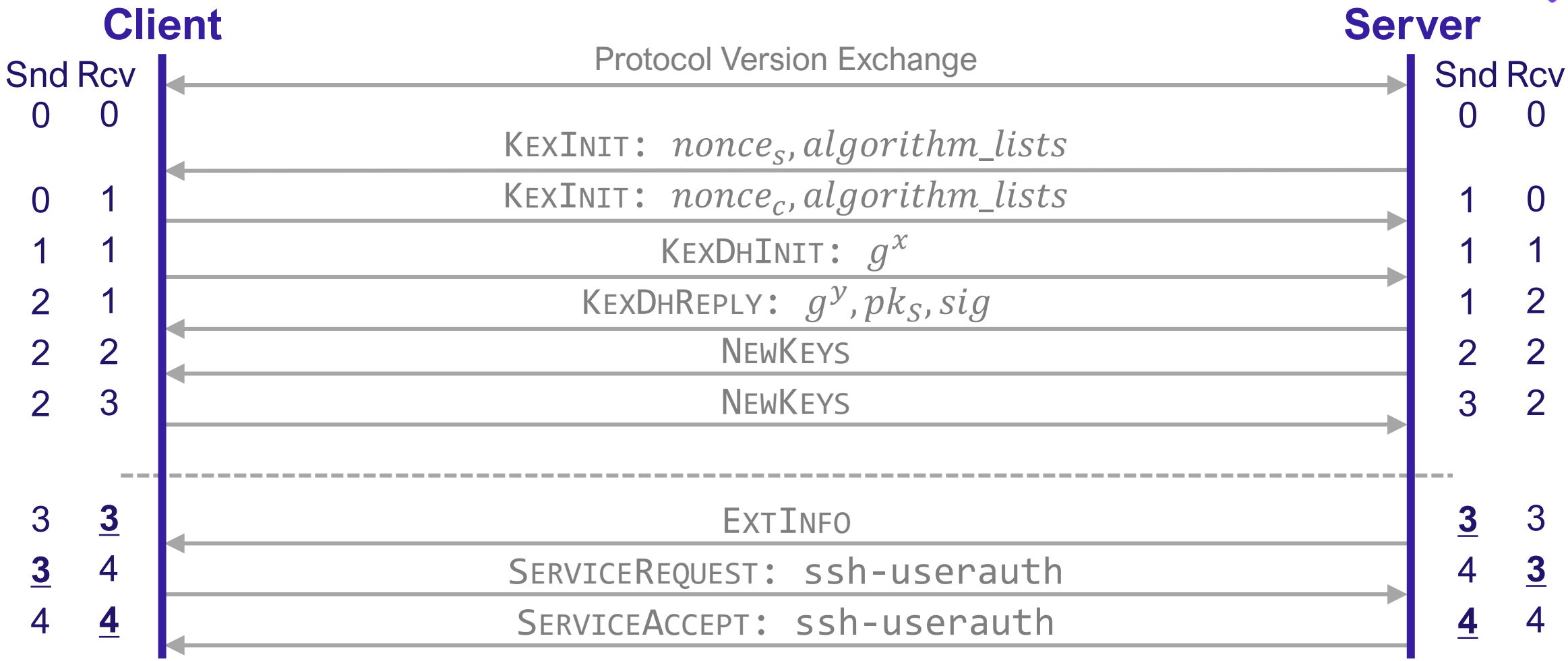
SSH Uses Implicit Sequence Numbers



SSH Uses Implicit Sequence Numbers



Introducing Sequence Numbers to the Flow



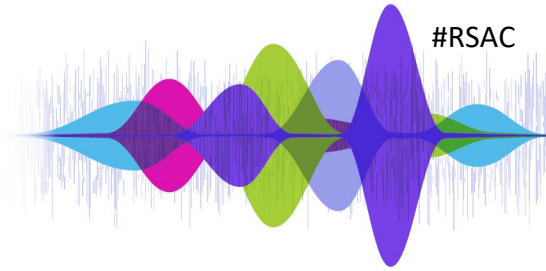
RSAC 2025 Conference

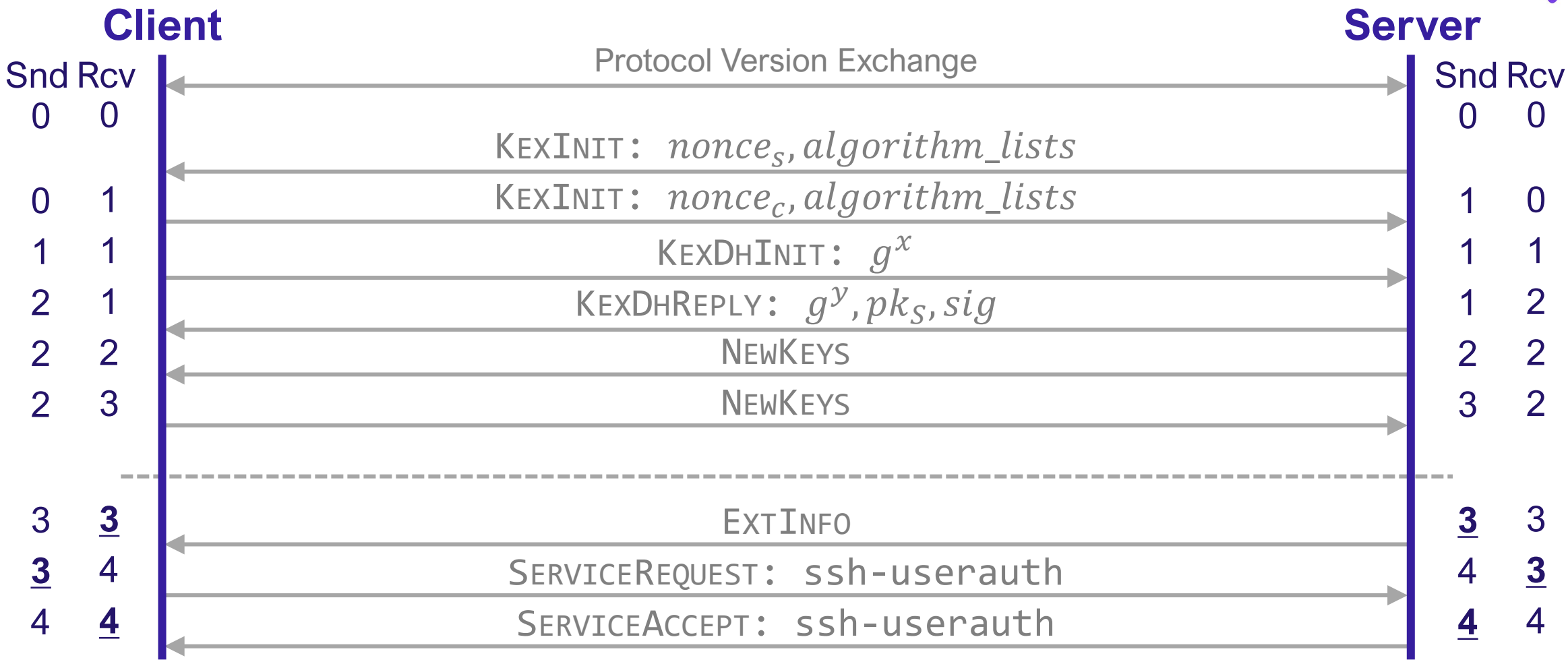
The Terrapin Attack

CVE-2023-48795
(CVE-2024-41909)

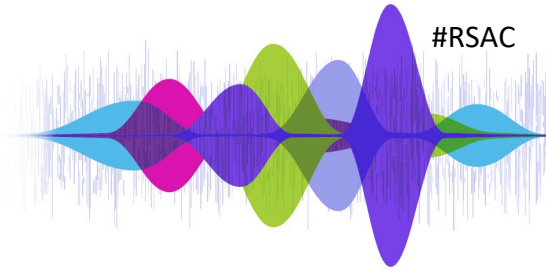
Many Voices.
One Community.

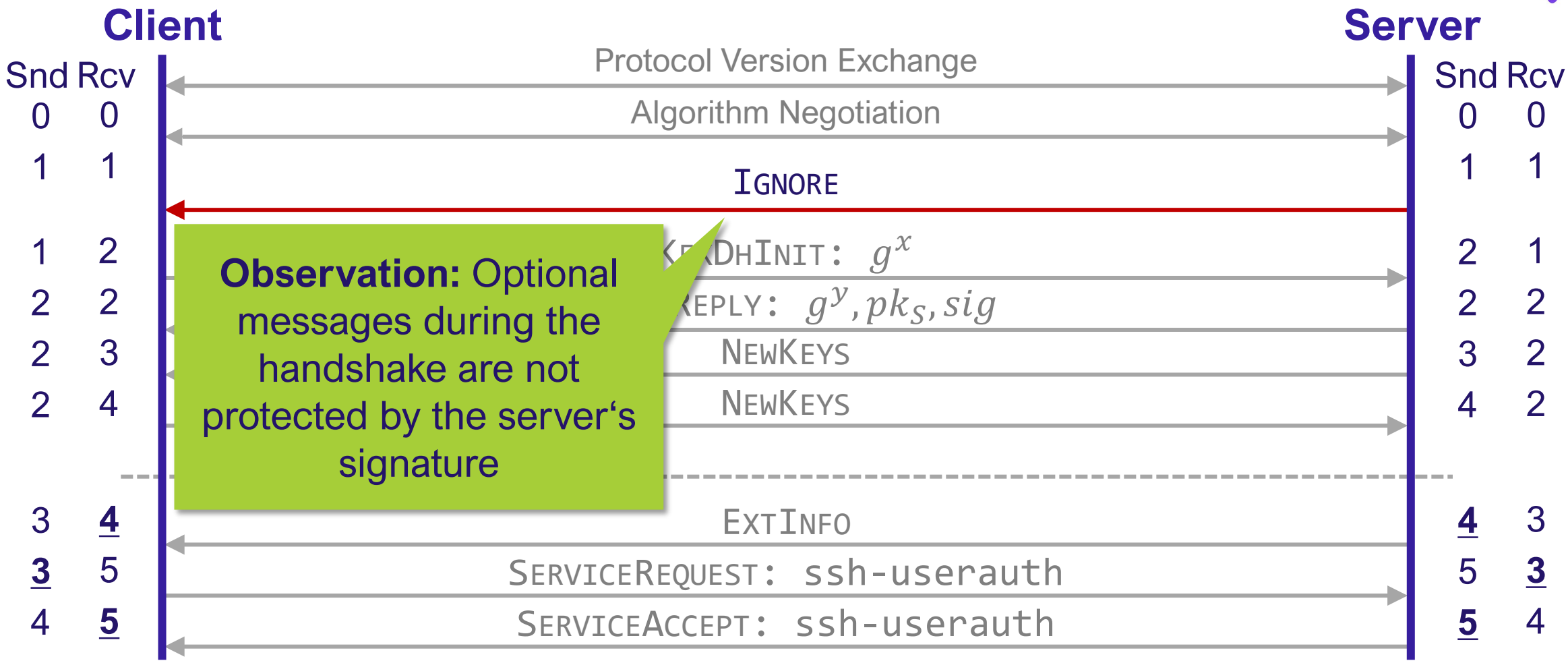
SSH Allows for Optional Messages in Handshakes



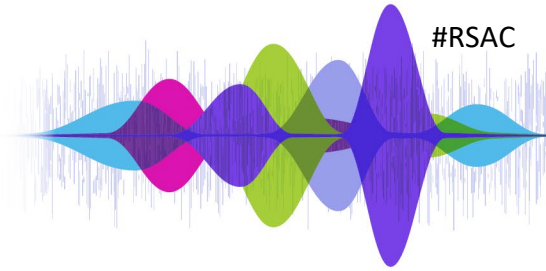


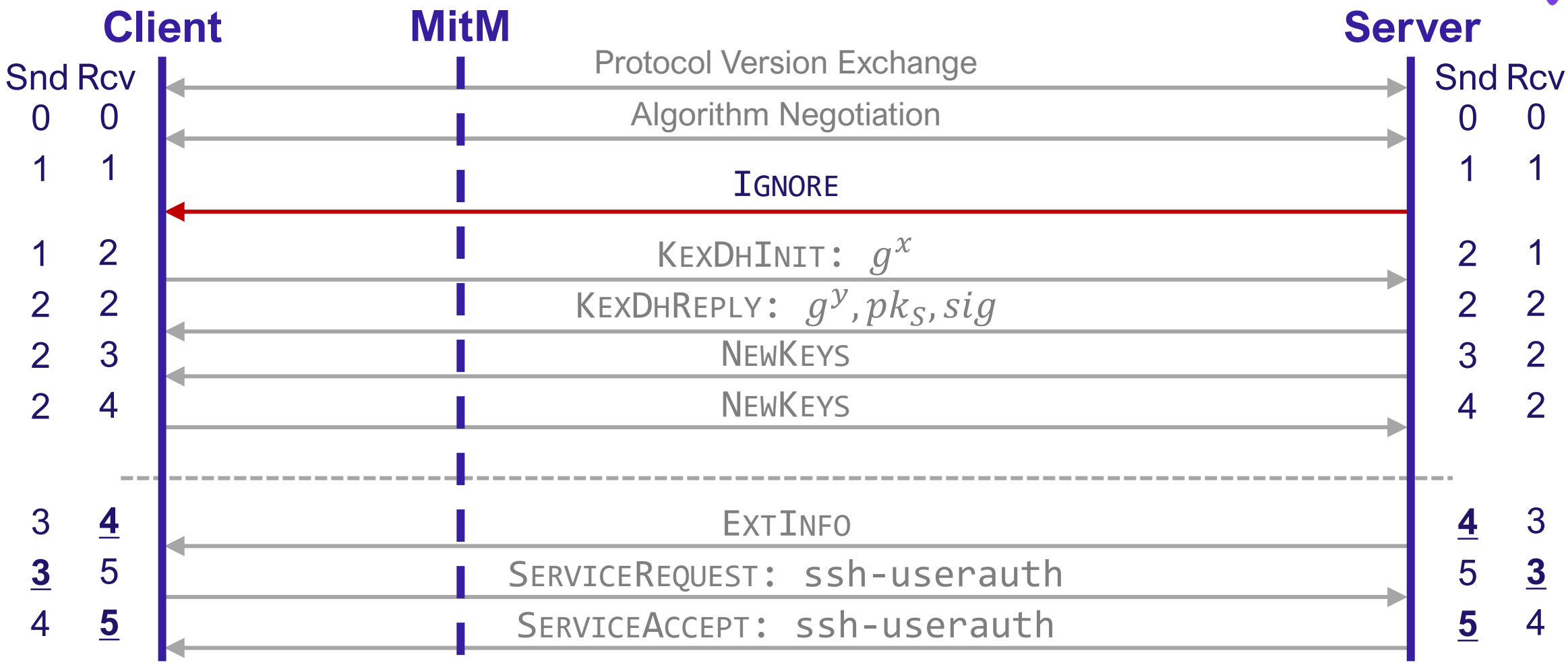
SSH Allows for Optional Messages in Handshakes



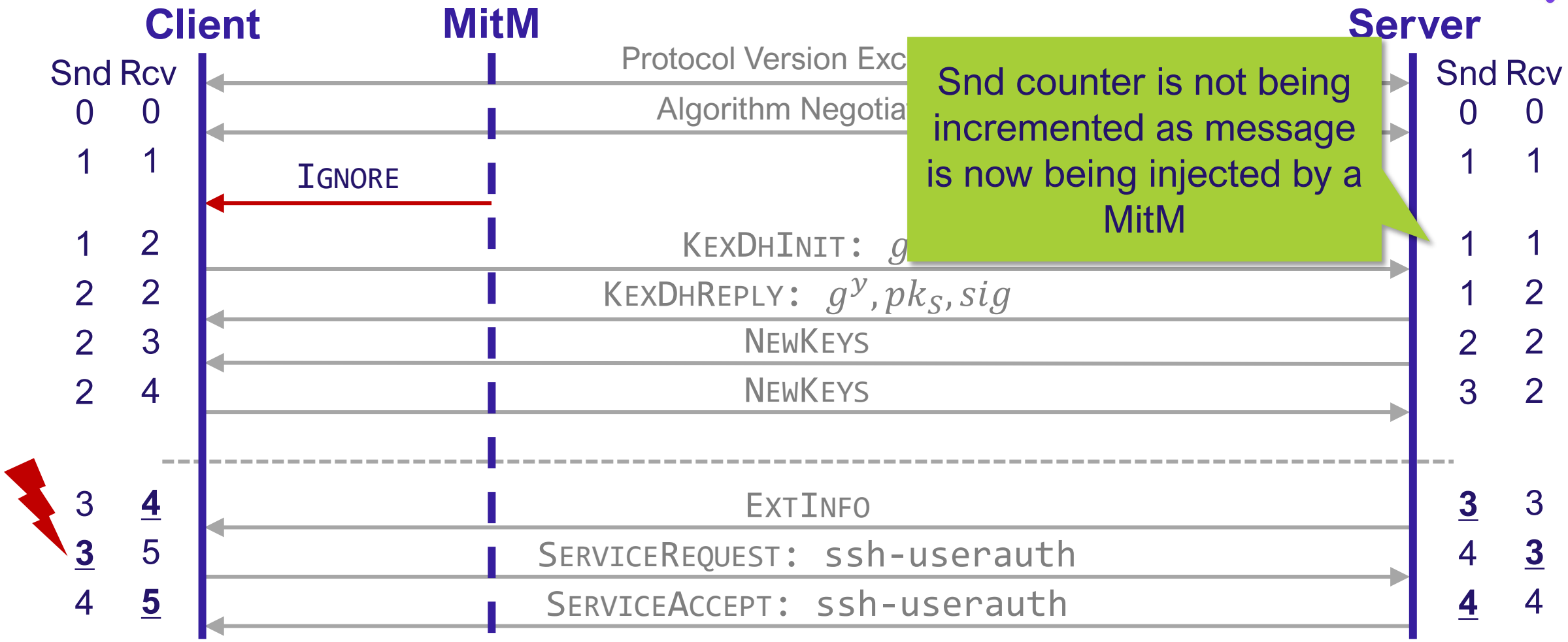


SSH Allows for Optional Messages in Handshakes

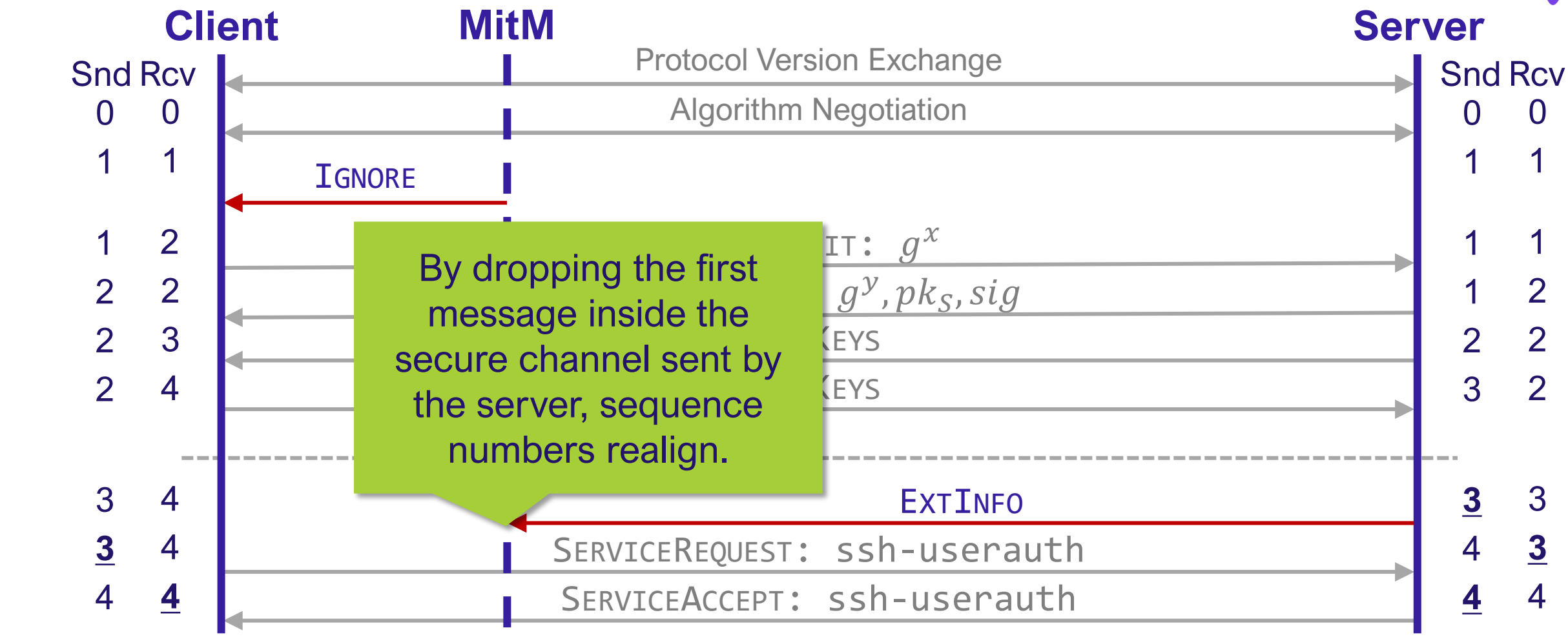




MitM Attackers Can Inject Messages Into Handshake…



… And Drop Messages Inside The Secure Channel



The ExtInfo Message Contains Extensions as Key-Value Pairs

server-sig-algs	ping@openssh.com	Other Extensions
• List of public key algorithms for user authentication • Enables RSA-SHA2 support	• Like Heartbeat extension in TLS • Can be used to obscure keystroke timings	• Not considered because no security impact

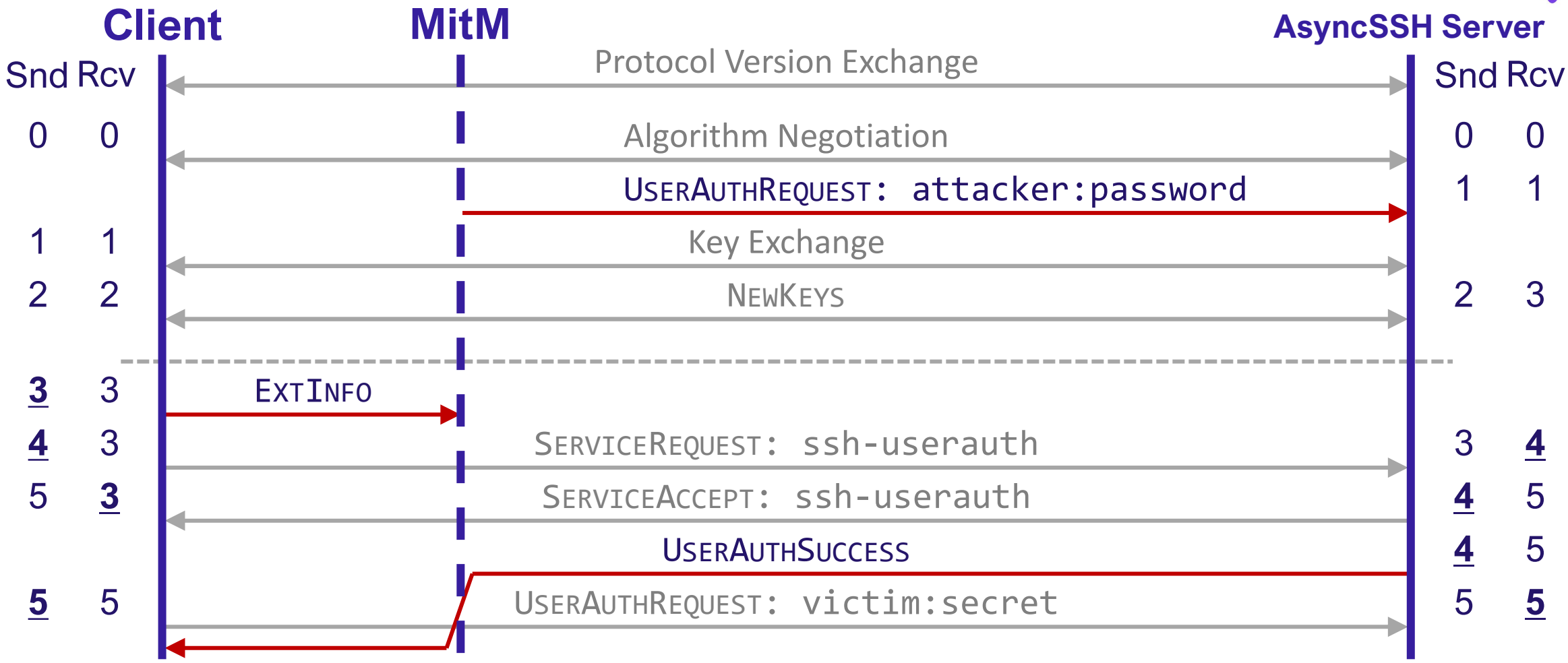
RSAC 2025 Conference

Implementation Bugs and Terrapin

CVE-2023-46445
CVE-2023-46446

Many Voices.
One Community.

Implementation Bugs Can Escalate Impact



RSAC 2025 Conference

Requirements and Countermeasures

ChaCha20-Poly1305 And Encrypt-then-MAC (EtM) Are Affected

Perfectly Exploitable

Exploitation Unlikely

Limited Exploitability

Success rate between 0.0003 – 0.8383

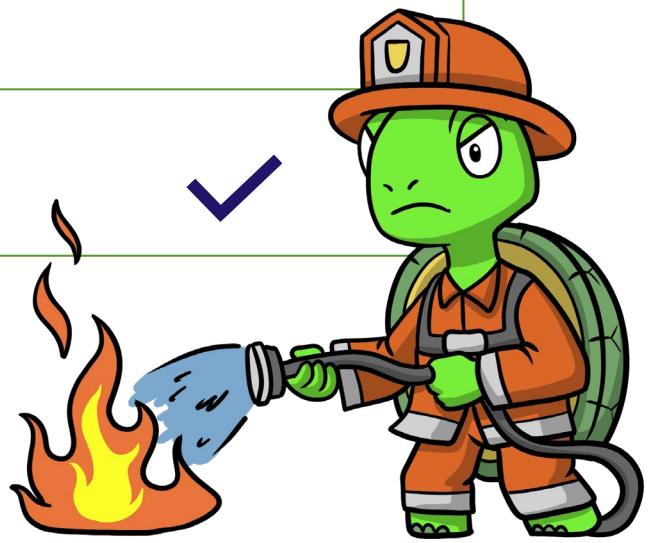
AE Mode	Preferred		Supported	
ChaCha20-Poly1305	8,739k	57.64%	10,247k	67.58%
CTR-EaM	3,964k	26.14%	4,200k	27.70%
GCM	1,219k	8.04%	10,450k	68.92%
CTR-EtM	828k	5.46%	10,685k	70.46%
CBC-EaM	359k	2.37%	1,585k	10.46%
CBC-EtM	14k	0.09%	2,614k	17.24%
Other	2k	0.01%	-	-
Unknown / No KEXINIT	36k	0.24%	-	-
Total	15,164k	100%		

Mitigating Our Attack Is Difficult

Countermeasure	Our Suggestion	"Strict KEX" (OpenSSH)
Reset sequence numbers at key installation	✓	✓
Authenticate the entire handshake transcript (hash)	✓	
Harden handshake to disallow unexpected messages		✓

> 30 unique implementations support "strict kex"

~ 11 million servers offer "strict kex"



Apply What You Have Learned Today

- Identify SSH servers in your organization
- Determine vulnerability to Terrapin and update accordingly
  - Basic vulnerability scanner available at https://terrapin-attack.com
  - No update available: Disable affected cipher modes
- Repeat this process for SSH clients!
  - Strict KEX requires support from client and server to take effect
  - A connection to a patched server can still be attacked if the client is vulnerable

RSAC 2025 Conference

Many Voices.
One Community.

Thanks! Questions?

For more information:

https://terrapin-attack.com